(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 643 475**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **89 02247**

(51) Int Cl⁵ : G 06 F 12/14.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 21 février 1989.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : BOPI « Brevets » n° 34 du 24 août 1990.

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *LIVOWSKY Jean-Michel.* — FR.

(72) **Inventeur(s)** : Jean-Michel Livowsky.

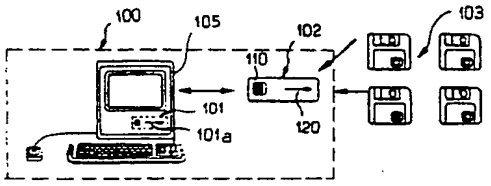
(73) **Titulaire(s)** :

(74) **Mandataire(s)** : Cabinet André Bouju.

(54) Procédé de contrôle de l'utilisation d'un support d'informations, notamment magnétique ou magnéto-optique et systèmes pour sa mise en œuvre.

(57) Le procédé de contrôle de l'utilisation d'un support d'informations 103 notamment magnétique ou magnéto-optique, sur un système de traitement d'informations 100 pourvu d'un code identifiant prédéterminé, comprend une étape d'association exclusive dudit support d'informations 103 audit système de traitement d'informations 100 de sorte qu'à l'issue de ladite étape, le support d'informations 103 est utilisable uniquement sur ledit système de traitement d'informations 100.

Utilisation pour contrôler l'utilisation de tous supports magnétiques ou magnéto-optiques, tels que disques, bandes, cassettes magnétiques ou magnéto-optiques de musique, de films et d'informations enregistrées.



FR 2 643 475 - A1

Vente des fascicules à l'IMPRIMERIE NATIONALE, 27, rue de la Convention — 75732 PARIS CEDEX 15

La présente invention concerne un procédé de contrôle de l'utilisation d'un support d'informations, notamment magnétique ou magnéto-optique. Elle vise également des systèmes pour sa mise en oeuvre.

La duplication et l'utilisation illicites de supports d'information, notamment des disquettes de programmes ou progiciels pour ordinateurs, ou de cassettes pour magnétoscopes, constituent actuellement un problème majeur pour les auteurs, éditeurs et distributeurs de ces supports d'information. Ces opérations frauduleuses en se généralisant mettent en péril économique des éditeurs qui consentent bien souvent de lourds investissements pour le développement et la mise au point des logiciels ou films enregistrés. Le développement très rapide du parc de micro-ordinateurs de magnétoscopes et de lecteurs de disques optiques dans le monde a largement amplifié le problème de l'utilisation non controlée des supports d'information, notamment magnétiques ou magnéto-optiques.

Pour endiguer cette situation à terme préjudiciable pour ce secteur économique, les auteurs et distributeurs de logiciels ont fait appel à de nombreux procédés existants de contrôle de l'utilisation de supports d'informations. Dans le domaine de la vidéo et des systèmes magnéto-optiques, la reproduction non autorisée du support est également endémique mais peu de moyens de protection ont été mis en place à ce jour. Ceux existants reprennent d'une manière plus simplifiée les systèmes de protection mis en place pour les logiciels.

On connait déjà des procédés visant à empêcher la duplication de données stockées sur des supports magnétiques ou magnéto-optiques par des "serrures" ou des verrous de comptage physiques et/ou logiques. La duplication de logiciels peut être ainsi gênée par la mise en place de protections numériques, logiques ou physiques telles que la réalisation d'un trou dans une piste. Cependant, les

protections numériques ou logiques peuvent être violés par l'utilisation de systèmes commercialisés librement et aucun système de protection de ce type n'offre une protection efficace des logiciels ou de tout autre support magnétique ou magnéto-optique. La plupart de ces systèmes ne permettent pas d'effectuer des copies de sauvegarde. Ils présentent en outre l'inconvénient de permettre la circulation des logiciels originaux avec leurs mots de passe entre plusieurs utilisateurs non autorisés. Ils sont souvent très coûteux.

D'autres procédés visent à interdire l'accès aux données stockées par l'utilisation de mots de passe et/ou de clefs logiques. Cependant, les informations circulant par voie numérique, il suffit en fait de décoder le programme ou logiciel protégé pour avoir accès aux codes et donc de les modifier, après par exemple, comparaison entre les listages de plusieurs versions originales du logiciel. Par ailleurs, le titulaire du programme peut en remettre une copie avec son mot de passe et en permettre ainsi la circulation frauduleuse.

On connaît déjà aussi un procédé de contrôle d'utilisation d'un support d'informations, appliqué au domaine de la micro-informatique, qui met en oeuvre pour chaque support (ou disquette) original, un dispositif de clef électronique qui doit être connecté sur un port d'entrée/sortie, de préférence un port série ou sur la carte contrôleur, du système de traitement d'informations concerné. A titre d'exemple, les clefs électroniques actuellement disponibles pour un utilisateur sur un micro-ordinateur, sont connectées sur un port de série RS 232. Ce procédé consiste à tester régulièrement la présence de cette clef grâce à des instructions spécifiques rajoutées au programme. Le programme ou logiciel ne peut donc être utilisé que sur des machines dotées de cette clef. Ce procédé permet à l'utilisateur de réaliser des copies de sauvegarde en nombre non limité. Il présente par contre l'inconvénient de

permettre la circulation du logiciel original avec sa clef électronique entre plusieurs utilisateurs sur différents micro-ordinateurs n'offrant alors qu'une protection relative. Il est par ailleurs possible, bien que coûteux, de dupliquer la clef physique. Par ailleurs, plusieurs systèmes identiques ne peuvent pas cohabiter simultanément. On ne peut pas travailler sur plusieurs programmes en même temps.

Par ailleurs, une clef électronique spécifique étant associée à chaque logiciel original, ce procédé nécessite une intervention matérielle de l'utilisateur pour connecter la clef électronique dans la partie appropriée du micro-ordinateur.

Le brevet français 2 579 790 divulgue ainsi un dispositif électronique de protection d'un accès notamment à un logiciel et une clef pour un tel dispositif.

D'autres procédés équivalents mettant en oeuvre une clef physique existent actuellement.

En particulier, le logimètre échange en permanence des informations avec le logiciel original et permet également un comptage des utilisations. Par ailleurs, son prix est hautement prohibitif. Ce procédé est pratiquement inviolable mais ne présente une solution fiable que vis à vis d'une seule machine.

Un autre procédé actuel de contrôle d'utilisation de support d'informations dans le domaine de la micro-informatique met en oeuvre un lecteur de cartes à mémoire connecté à un ordinateur ou micro-ordinateur. Une carte à mémoire comportant un microprocesseur sécurisé associée au logiciel protégé contient des algorithmes spécifiques qui permettent de vérifier et de comptabiliser l'utilisation du logiciel. Le brevet français 2 266 222 divulgue par exemple un procédé et dispositif de commande électronique permettant d'obtenir de telles cartes à mémoire. Ce procédé de contrôle d'utilisation, qui nécessite un lecteur de cartes à mémoire, est coûteux, présente aussi l'inconvénient précité de ne pas

limiter l'utilisation d'un logiciel à un ordinateur ou micro-ordinateur unique et rend ainsi possible l'utilisation du logiciel sur d'autres systèmes équipés d'un lecteur de cartes à mémoire, pour peu que l'on dispose de la carte associée au logiciel. Un autre procédé consiste à inscrire une partie du programme sur la carte qui ne peut fonctionner qu'avec son mot de passe ou son code.

Ainsi, l'ensemble des procédés existants de contrôle d'utilisation n'offre qu'une protection relative dans la mesure où ces procédés n'empêchent pas l'utilisation du logiciel original protégé sur un autre système de traitement, si l'utilisateur non autorisé dispose aussi de la clef électronique ou de la carte-mémoire. Ils ne procurent pas une protection absolue qui n'autoriserait l'utilisation d'un support d'information que sur un système de traitement unique tout en offrant au détenteur la possibilité de la dupliquer à volonté

En règle générale,

- tout système logiciel de protection est duplicable, ce qui permet donc de dupliquer les données complètes et de faire circuler des copies illicites,
- toute clef ou code d'utilisation peut être communiqué à un tiers,
- les clefs logiques et physiques font appel à des techniques très coûteuses.

On peut aussi faire circuler librement le logiciel et sa clef.

Ainsi, les grands distributeurs de programmes informatiques enregistrés ont été contraints d'abandonner tout procédé de protection et ont en revanche augmenté de façon sensible le prix de leurs programmes, faisant payer le prix des duplications illicites aux utilisateurs acquittant leur licence.

Le but de l'invention est de remédier à ces inconvénients en proposant un procédé de contrôle de

l'utilisation d'un support d'information, notamment magnétique ou magnéto-optique, sur un système de traitement d'informations pourvu d'un code identifiant prédéteminé.

Suivant l'invention, le procédé comprend une étape d'association exclusive du support d'information au système de traitement d'informations de sorte qu'à l'issue de ladite étape, le support d'informations est utilisable uniquement sur ledit système de traitement d'informations.

Ainsi, avec le procédé selon l'invention, à chaque support d'information protégé, correspond un système de traitement d'informations associé unique et exclusif, qui peut d'ailleurs être constitué parun réseau de systèmes. Le support ne peut alors être utilisé que dans ce système de traitement et lui seul. Par ailleurs, aucune restriction à la duplication du support n'est a priori nécessaire, permettant ainsi à l'utilisateur autorisé dudit support de bénéficier d'une protection absolue, -son support ne peut être utilisé que sur un système de traitement précisément identifié-, tout en n'étant pas limité dans la duplication du support original pour réaliser des copies de sauvegarde.

Le procédé selon l'invention permet donc de contourner efficacement toutes les difficultés connues propres aux systèmes de protection existants, en augmentant la sécurisation des données et des programmes de façon inégalée.

Il ne nécessite pas l'introduction par l'utilisateur d'un code ou d'un mot de passe, ne fait pas appel à une clef physique, souvent coûteuse et de plus transportable, et n'apporte aucune restriction à la duplication du support par l'utilisateur autorisé.

Suivant un mode préféré de réalisation de l'invention, l'étape d'association exclusive comporte une étape de transfert d'une information codée d'identification, générée à partir du code identifiant du système de traitement d'informations, depuis le système de traitement

d'informations vers le lecteur qui après l'avoir encodée l'inscrit dans une zône prédéteminée du support d'informations. Ainsi, à l'issue de cette étape de transfert, le support d'informations possède en son sein une information d'identification du système de traitement d'informations auquel le support a été initialement associé. La détention de cette information d'identification au sein du support permet de pouvoir identifier univoquement le système de traitement d'informations sur lequel une utilisation dudit support est autorisée. Le support est ainsi à l'aide de son lecteur virtuellement capable de se situer géographiquement dans son propre environnement de traitement d'informations. Aucune protection de duplication n'est nécessaire pour assurer une protection absolue des informations stockées sur le support.

De façon avantageuse, le procédé comprend, pour chaque tentative d'utilisation d'un support d'information sur le système de traitement d'informations, une série d'étapes de test de conditions d'utilisation au cours de laquelle est vérifiée l'existence d'une information codée de support au sein de la zône prédéterminée associée au support d'informations, et dans le cas où elle existe, cette information codée de support est comparée à l'information codée d'identification.

De cette façon, un système de traitement d'informations lié à son lecteur mettant en oeuvre ce procédé es d'identifier la présence d'une information codée au sein du support d'informations, permettant ainsi d'autoriser ou d'interdire l'utilisation de ce support sur le système de traitement d'informations concerné, suivant la programmation de la zone prédéterminée, en fonction de la licence associée au support d'informations.

Suivant un autre aspect de l'invention, le système de contrôle de l'utilisation d'un support d'informations, notamment magnétique ou magnéto-optique sur un système de

traitement d'informations, mettant en oeuvre le procédé pourvu de moyens d'identification selon l'invention, comprend des moyens pour associer exclusivement ledit support d'informations audit système de traitement d'informations de sorte que ledit support d'information soit utilisable uniquement sur ledit système de traitement d'informations, lesdits moyens d'association exclusive étant répartis dans le support d'informations et dans le système de traitement d'informations.

Ainsi, chaque support d'information ainsi protégé dispose de moyens permettant d'identifier le système de traitement d'informations associé et, un système de traitement d'informations mis en oeuvre dans l'invention peut être choisi comme environnement hôte d'un support d'information donné.

Suivant une forme de réalisation avantageuse de l'invention, le système de traitement d'informations comprend, au titre des moyens d'association exclusive, des moyens pour transférer sélectivement une information codée d'identification, issue des moyens d'identification et traitée préalablement par des moyens encodeurs inclus dans ledit système de traitement d'informations, vers une zône prédéterminée dudit support d'informations.

Il est à noter que des moyens d'identification complémentaires peuvent être extérieurs au système de traitement d'informations et être notamment, un détecteur d'empreintes digitales, d'empreintes vocales ou bien un analyseur irridologique.

D'autres particularités et avantages de l'invention apparaîtront encore dans la description ci-après.

Aux dessins annexés donnés à titre d'exemples non limitatifs :

- la figure 1 est une vue schématique simplifiée des principaux éléments mis en oeuvre dans une version du procédé conforme à l'invention,

- la figure 2 est une vue schématique d'une forme particulière d'un lecteur d'un système de traitement d'informations mis en oeuvre dans un système de contrôle d'utilisation selon l'invention ;

- la figure 3 illustre une forme de réalisation particulière d'un support d'informations constitué d'une disquette standard à laquelle est fixée un circuit intégré programmable ;

- la figure 4A est une première partie de l'organigramme d'une version du procédé conforme à l'invention ;

- la figure 4B est une seconde partie de l'organigramme 4A.

- la figure 5 est un schéma synoptique illustrant les fonctions d'encryptage et de décompaction mises en oeuvre dans le procédé selon l'invention.

On va maintenant décrire de façon détaillée une forme particulière de réalisation d'un système de contrôle d'utilisation selon l'invention, appliqué au cas d'un micro-ordinateur et de supports d'informations magnétiques sous la forme de disquettes, en référence à la figure 1.

Le système de traitement d'informations 100 comprend un micro-ordinateur 105 de type connu doté d'un lecteur de disquette qui peut être interne 101 ou externe 102. Suivant l'invention, le lecteur 101 ou 102 comprend un lecteur de données sur support magnétique 120 et un lecteur de microcalculateur 110 représenté symboliquement par la référence 110 sur le schéma de la figure 1. Les disquettes supports d'information 103 comportent, dans un boîtier standard, un disque magnétique de stockage et sur une de leurs faces latérales extérieures, un circuit intégré de type microcalculateur ou microprocesseur, comme on le décrira plus en détail plus loin. On peut envisager comme support d'informations aussi bien l'utilisation d'un disque optique ou magnéto-optique, réinscriptible ou non.

La figure 2 illustre de façon très simplifiée les différents composants d'un lecteur 60 pouvant équiper un système de traitement d'informations 100, tel qu'un micro-ordinateur intervenant dans un système de contrôle d'utilisation selon l'invention. Le lecteur 60 comprend tout d'abord un lecteur de données numériques 61 de type standard, permettant en général d'effectuer les deux fonctions de lecture et d'écriture sur un support magnétique, tel qu'une disquette, préalablement introduit dans la fente appropriée 101a du lecteur 101 du micro-ordinateur 105. Au lecteur de données numériques 61 sont associés un module de gestion des insertions de disque 66 et une mémoire de zones de programmes 65. Le lecteur 60 comprend en outre un dispositif 69 de lecture/écriture de circuits intégrés programmables fixés, conformément à l'invention, aux supports d'information, dans le cas présent, les disquettes. Une mémoire vive 64, de type RAM, est associée à ce dispositif de lecture/écriture 69 de codage et est destinée à recevoir une information codée d'identification du système de traitement d'informations, dans le cas présent, le micro-ordinateur 105.

Le lecteur 60 comprend en outre à cet effet, un module 63 de recherche d'un identifiant du micro-ordinateur, au sein de zones mémoires prédéterminées de celui-ci, et un module électronique 62 inviolable d'encodage de l'identifiant pour générer l'information codée d'identification.

Par ailleurs, les fonctions d'encryptage/désencryptage et/ou de décompaction sont assurées respectivement par un module 67 d'encryptage/désencryptage et/ou un module 68 de décompaction qui intègrent tous deux des protocoles stockés en mémoire.

Il est à noter que l'encryptage est un procédé connu de protection par lequel on insère dans une suite

numérique donnée, représentant indifféremment un programme ou des données, un code extérieur étranger aux données stockés. Par ailleurs, le compactage est un procédé connu de réécriture des algorithmes de données permettant de réduire après l'opération de compactage, l'encombrement physique d'une suite de données sur un support. Le gain de place peut atteindre 70 %. Le désencryptage et la décompaction sont les opérations inverses respectives de l'encryptage et du compactage.

Ces deux principes combinés, encryptage et compactage, permettent de faire circuler des données ou des programmes librement, en maintenant la confidentialité et en réduisant leur encombrement. Le principe connu permet donc de décompacter un programme donné après avoir fourni un code d'accès ou une clef au programme de décompaction. La mise en oeuvre originale de ces principes dans le procédé selon l'invention sera décrite plus en détail dans la suite.

Dans une forme de réalisation particulière de l'invention et non limitative, des disquettes 50 (voir figure 3), considérées comme supports d'information, sont munies sur une de leur face externe, d'un circuit intégré 51, du type de ceux équipant les cartes bancaires ou multiservices. Le circuit intégré ou microcircuit 51 est nécessairement accessible en écriture et en lecture et comporte de préférence un microprocesseur ou un microcalculateur sécurisé. Chaque disquette 50 comprend alors deux supports d'information fonctionnellement indépendants mais solidaires,l'un consistant en un support magnétique 52 d'informations numériques (données ou logiciel) et l'autre étant le microcalculateur 53 qui a pour fonction de contenir et traiter des informations codées échangées avec la partie de codage du lecteur 60.

On va maintenant décrire en détail le procédé selon l'invention en même temps que le système conforme à l'invention appliqué au contrôle de l'utilisation de

supports magnétiques tels que des disques souples, sur un micro-ordinateur 100 équipé d'un lecteur 60 tel que décrit précédemment, en référence à l'organigramme représenté aux figures 4A et 4B.

On suppose tout d'abord que le micro-ordinateur 100 est doté d'un identifiant stocké dans une mémoire ROM.

Une première phase 1 du procédé selon l'invention consiste à transférer et à coder cet identifiant depuis la mémoire ROM dans la mémoire vive 64 du lecteur 60 qui peut être soit inclus dans le micro-ordinateur, soit extérieur à celui-ci, comme cela est bien connu dans le domaine de la micro-informatique.

A la mise sous tension 2 du micro-ordinateur, le lecteur 60 est activé (étape 3) et le module 63 de recherche de l'identifiant est mis en oeuvre pour aller lire celui-ci dans la mémoire ROM du micro-ordinateur (étape 4). Une étape 5 de codage de l'identifiant est alors effectuée au cours de laquelle le module électronique encodeur 62 inviolable est mis en oeuvre. L'information codée d'identification ainsi obtenue est ensuite inscrite (étape 6) dans la mémoire RAM 64 du lecteur 60.

Après introduction 10 d'un support 103 dans le lecteur 60, 120 du micro-ordinateur, une étape 11 de vérification de l'existence d'un micro-calculateur ou d'un micro-processeur est effectuée, mettant en oeuvre le dispositif d'écriture/lecture de codage 69. Il s'agit de déterminer si le support qui vient d'être introduit dans le lecteur est effectivement doté de moyens de contrôle d'utilisation. Si ce n'est pas le cas, le lecteur 60 prend en compte le support et assure les échanges classiques d'informations (données, logiciels) entre le support et l'unité centrale du micro-ordinateur (étape 13), dans le cadre du fonctionnement normal d'un lecteur de ce type.

Dorénavant, on employera les termes respectifs de microcircuit pour désigner l'ensemble du circuit fixé sur la

disquette support d'information, et de microprocesseur pour désigner le composant programmable, qui peut être un composant programmable accessible en lecture et en écriture, mis en oeuvre dans l'invention.

Dans le cas d'une détection effective d'un microprocesseur, l'existence d'un code au sein du microcalculateur est testée par les moyens d'écriture/lecture de codage 69 du lecteur 60, au cours d'une étape 12. L'absence de code implique que le microprocesseur est vierge (étape 10) et conduit à la phase 17 de procédure de première installation.

La présence d'un code dans le microprocesseur conduit à une étape 15 de comparaison avec un ou plusieurs codes interdits éventuellement présents dans une zone de mémoire du microprocesseur. Cette zone de mémoire d'inscription de codes interdits est nécessairement sécurisée et absolument non modifiable, conformément au principe connu de sécurisation des microprocesseurs. Les codes interdits correspondent aux codes d'identification éventuellement inscrits dans le microprocesseur au cours de précédentes installations du support d'informations, ce qui sera expliqué plus en détail dans la suite. La détection d'un code interdit conduit classiquement à une procédure 14 d'éjection ou de rejet de la disquette support ou de fonctionnement restreint ou partiel du programme, par exemple, à des fins de démonstration commerciale.

Dans le cas contraire, le code support détecté est comparé (étape 18) à l'information codée stockée dans la mémoire vive 64 du lecteur 60. Une égalité entre les deux codes conduit naturellement à un fonctionnement normal 19 du lecteur 60 vis à vis des données stockées sur le support. En effet, le support d'informations concerné, dans le cas présent la disquette qui vient d'être introduite dans le lecteur, se trouve mis en relation avec le micro-ordinateur du système de traitement d'informations auquel elle a été

préalablement associée de façon exclusive.

Dans le cas d'une différence entre les deux codes respectivement stockés dans la mémoire vive 64 du lecteur 60 et dans la mémoire microprocesseur 51 de la disquette 50, une phase 23 d'éjection/rejet de la disquette ou de fonctionnement restreint est mise en oeuvre.

Il peut être prévu optionnellement une procédure 22 de désinstallation/réinstallation au cours de laquelle, d'une part, le code actuellement présent dans la mémoire du microprocesseur du support est stocké dans une pile dans ladite mémoire (étape 20), ce code devenant alors un "code interdit", et, d'autre part, le code de support du microprocesseur est réinitialisé, permettant alors d'entreprendre une nouvelle procédure d'installation 17, le microprocesseur étant alors reconnu par le lecteur 60 comme vierge. Il peut être prévu par la licence d'utilisation un nombre prédéterminé de réinstallations possibles pour un même support. Ceci peut par exemple permettre, contrairement aux systèmes de protection de l'art antérieur, la libre circulation de programmes complets avec leur documentation intégrale, le système de comptage intégré dans le microprocesseur n'autorisant un système de traitement d'informations donné qu'à accepter un nombre restreint de fois un programme, et encourageant donc la circulation du programme complet entre de multiples utilisateurs, uniquement à des fins de promotion commerciale.

La procédure de première installation est illustrée sous forme d'organigramme en figure 4B, où la référence A désigne le point de liaison entre les deux parties d'organigrammes représentées respectivement en figures 4A et 4B, pour des raisons de taille. Cette procédure comporte une étape d'association exclusive 30 du support (disquette) au cours de laquelle l'information codée d'identification est inscrite dans la mémoire du microprocesseur du support. Il est prévu ensuite une étape

31 de détermination du contenu du support. S'il s'agit de données (ou datas), la nécessité optionnelle d'une clef logicielle spécifique à l'utilisateur est testée (étape 33), conduisant soit au libre accès 32 aux données stockées sur le support, soit à l'introduction 36 de la clef par l'utilisateur du micro-ordinateur.

Celle-ci est vérifiée (étape 37), la vérification conduisant soit à l'éjection ou au rejet de la disquette support (étape 39), soit au fonctionnement normal du lecteur 60 en lecteurs de données (étape 38). Cette "clef utilisateur" fonctionne selon les procédés connus d'encodage/encryptage d'une série alphanumérique dans une suite logique donnée. Elle peut être renforcée par l'inscription de ladite clef dans le microprocesseur, assurant l'inviolabilité du code.

Si le contenu du support consiste en un logiciel, un projiciel, ou plus généralement, ce qui est d'ordinaire désigné par ressources, un premier test 40 pour déterminer si le programme est ouvert à un encryptage est réalisé. Si c'est le cas, une procédure 41 d'inscription par ensemencement et enrelacement du code dans la structure logicielle du programme est effectuée.

Quel que soit le résultat du test d'encryptage 40, un second test 42, 48 pour déterminer si le programme est ouvert à une décompaction est effectué.

Si le programme concerné est à la fois crypté et ouvert à décompaction, une étape 43 de décompaction et d'installation sur un disque dur ou tout autre dispositif de stockage permanent du système de traitement d'information est effectuée, ce qui se traduit, en fonctionnement normal du système, par une série d'étapes d'échange permanent d'informations et de codes entre le programme et la mémoire RAM 64 du lecteur 60.

La figure 5 illustre schématiquement les phases essentielles d'inscription du code par ensemencement et

entrelacement et de décompaction, mises en oeuvre dans le système selon l'invention appliqué au contrôle de l'utilisation de logiciels/

I : Le programme présent sur la disquette support est initialement dans un état compacté 200, et est prêt à être ensemencé. Les parties 202 du programme 200 est normalement compactée tandis que les parties 201 sont destinées à l'ensemencement d'un code XXX, 211, présent dans le microprocesseur associé au support.

E : au cours de la procédure 41 d'inscription, le code 211 est effectivement introduit et dupliqué dans les parties appropriées du programme qui présente alors un état compacté et ensemencé 210.

D : à l'issue de l'étape 43 de décompaction et d'installation, les codes 211 se trouvent entrelacés dans le programme à l'état décompacté 220. Or, les "sommes de vérification" ou "check-sum" de ligne 221 sont contrôlées régulièrement, ce qui se traduit par l'impossibilité de changer le code 211 sans invalider le programme. En effet, si le code 211 change, alors les "check-sum" changent et le programme ne peut plus fonctionner. Lors de chaque étape d'échange permanent entre le programme et la mémoire RAM 64 du lecteur 60 qui stocke notamment le code présent en mémoire du microprocesseur. S'il y a différence, le programme se bloque.

Si le programme concerné est crypté mais n'est pas ouvert à décompaction, le fonctionnement du programme ou logiciel est autorisé directement à partir du lecteur 60 sur son support (étape 44). Une clef logicielle de comptage est optionnellement prévue afin de fixer un nombre prédéterminé d'utilisations du logiciel, suivant les opportunités techniques ou commerciales. Le système de comptage peut être installé dans une zone appropriée du microprocesseur.

Dans le cas où le programme n'a pas été crypté, celui-ci peut être, soit décompacté et installé sur le

disque dur ou un dispositif de stockage permanent équivalent, éventuellement muni d'une clef logicielle de blocage (étape 47), soit être utilisé directement à partir du lecteur de données 60, éventuellement muni d'une clef de comptage (étape 49).

Une autre particularité de l'invention est de permettre la désinstallation optionnelle d'un programme ou logiciel. En effet, si l'information codée d'identification inscrite dans le microcalculateur ne peut être effacée, il est toutefois possible par une fonction logicielle appropriée de permettre la désactivation de la reconnaissance de l'information codée pour la remplacer par une autre dans le cas d'une nouvelle procédure complète d'installation du code. Dans ce cas, comme cela a été décrit précédemment,l'information codée initiale est cependant conservée dans une zone mémoire sécurisée et totalement non modifiable et devient un code interdit, comme décrit précédemment. Cette option permet à l'utilisateur de pouvoir changer de système de traitement hôte, en cas par exemple de destruction de la carte mère du micro-ordinateur, de changement de numéro de téléphone dans le cas d'un terminal de télécommunications faisant fonction de système de traitement, ou en cas de vente ou cession du logiciel.

Le procédé selon l'invention présente en outre l'avantage de pouvoir être automatisé aisément, en réduisant au minimum toute intervention de l'utilisateur. En effet, à la différence de systèmes de protection combinant un support de logiciel et une carte électronique physiquement distincts, le système selon l'invention associe étroitement les deux éléments que sont le support et le microprocesseur et comprend un système de lecture combinée de ces deux éléments.

Un autre avantage de l'invention est que celle-ci peut être mise en oeuvre dans un contexte d'utilisateurs multiples, au sein d'un réseau de micro-ordinateurs par exemple. Il suffit que tous les ordinateurs ou micro-

ordinateurs du réseau soient sous tension lors de la première introduction d'une disquette support originale dans le lecteur de l'un d'entre eux. Les valeurs reconnues pour chaque système deviennent alors combinatoires dans le cadre d'une vérification de réseau de type "check sum" mais l'invention ne perd pas pour autant son caractère de protection absolue.

Le système de traitement d'informations au regard de l'invention est alors constitué :

- soit par l'un des postes du réseau de micro-ordinateurs,
- soit par un nombre prédéterminé des postes du réseau,
- soit par l'ensemble des postes du réseau.

Ceci dépend essentiellement de la programmation préalable du microprocesseur sécurisé du support d'informations, qui est la traduction numérique de la licence commerciale associée audit support.

Bien entendu, l'invention n'est pas limitée aux exemples décrits et représentés et de nombreux aménagements peuvent être apportés à ces exemples sans sortir du cadre de l'invention.

Ainsi, n'importe quel système de traitement d'informations, y compris des terminaux de type videotexte, ASCII, télétype, VT52 ou équivalents pour peu qu'il soit doté d'un identifiant extérieur au lecteur, peut être équipé du système de contrôle d'utilisation selon l'invention.

L'identifiant peut être constitué d'une série d'informations permanentes qui peuvent être par exemple le numéro de la carte mère d'un micro-ordinateur, ou bien, dans le cas d'un terminal de télécommunications, le numéro de téléphone de la ligne auquel est raccordé le terminal, obtenu en utilisant par exemple un principe connu de reconnaissance de ligne PTT (3644 retour-retour).

Le support d'informations peut être inscriptible

ou non, comme dans le cas de supports de type CD-ROM et l'invention est applicable à tous supports de données magnétiques, magnéto-chimiques, notamment les mémoires à bulle, optiques ou magnéto-optiques tels que, mais non limitativement, disques et disquettes de tous formats et de toutes capacités, bandes magnétiques de tous formats et de toutes capacités, y compris les bandes magnétiques de stockage vidéo et les bandes de stockage de type magnétophone à cassettes, ainsi qu'à des supports d'informations mettant en oeuvre des circuits bioélectroniques ou électro-chimiques.

L'invention peut aussi s'appliquer à des supports d'informations couplés à des moyens de transport de ces informations non matériels, tels que des faisceaux optiques ou des flux de données dans un canal hertzien ou galvanique, par exemple dans le cas des transmissions par modulateur-démodulateur (modem).

On peut aussi envisager, dans le cadre de l'invention, un support d'informations constitué par un disque magnétique dont un nombre prédéterminé de pistes serait formaté selon un premier procédé de formatage et dont les autres pistes seraient formatées selon un second procédé de formatage, ce qui éviterait d'avoir recours à un module spécifique de stockage des informations confidentielles de code actif et de codes interdits, se trouvant solidaire de l'enveloppe matérielle du support d'informations tel que décrit dans l'exemple préférentiel de la présente invention.

REVENDICATIONS

1. Procédé de contrôle de l'utilisation d'un support d'informations (103, 50), notamment magnétique ou magnéto-optique, sur un système de traitement d'informations pourvu d'un code identifiant prédéterminé, caractérisé en ce qu'il comprend une étape d'association exclusive dudit support d'informations (103) audit système de traitement d'informations (100) de sorte qu'à l'issue de ladite étape, ledit support d'informations (103) est utilisable uniquement sur ledit système de traitement d'informations (100).

2. Procédé selon la revendication 1, caractérisé en ce que l'étape d'association exclusive comporte une étape de transfert (30) d'une information codée d'identification générée à partir du code identifiant du système de traitement d'informations (100) depuis le système de traitements d'informations (100) dans une zône prédéterminée (51) du support d'informations (50).

3. Procédé selon la revendication 2, caractérisé en ce qu'il comprend, pour chaque tentative d'utilisation d'un support d'informations (50) sur ledit système de traitements d'informations (100) une étape de test de conditions d'utilisation (11, 12) au cours de laquelle l'existence d'une information codée de support au sein de la zone prédéterminée (51) dudit support d'informations (50) est vérifiée, et si elle existe, cette information codée de support est comparée à l'information codée d'identification.

4. Procédé selon la revendication 3, caractérisé en ce que, pendant l'étape de test de conditions d'utilisation (11, 12), la détection d'une absence d'informations codées de support au sein de la zône prédéterminée dudit support d'informations conduit à l'étape initiale d'association exclusive (A).

5. Procédé selon l'une des revendications 3 ou 4, caractérisé en ce que, pendant l'étape de test des conditions d'utilisation (11, 12), la détection après

comparaison d'une égalité entre l'information codée de support et l'information codée d'identification conduit à une étape d'utilisation normale (19) du support d'information sur le système de traitement d'informations.

6. Procédé selon l'une des revendications 2 à 5, appliqué au contrôle de l'utilisation d'un support d'informations numériques, notamment logicielles, caractérisé en ce qu'à l'issue de l'étape de transfert (30) d'une information codée d'identification, l'étape d'association exclusive comprend en outre une étape (31) pour déterminer si les informations contenues dans ledit support (103, 50) correspondent, soit à des données, soit à un logiciel.

7. Procédé selon la revendication 6, caractérisé en ce que dans le cas d'une détermination d'informations numériques correspondant à un logiciel, l'étape de détermination (31) est suivie d'une étape de détection d'encryptabilité (40) dudit logiciel, conduisant en cade de détection effective, à une étape d'inscription (41) de ladite information codée d'identification par entrelacement avec les informations numériques contenues dans le support d'informations (103, 50).

8. Procédé selon la revendication 7, appliqué à un système de traitement d'informations numériques comprenant un dispositif de stockage permanent d'informations, notamment un disque dur, caractérisé en ce que l'étape d'association exclusive (A) comprend en outre une étape (42, 48) pour déterminer si le logiciel est ouvert à une procédure de décompaction suivie en cas de détection, d'une étape de décompaction (43, 49) dudit logiciel et d'une étape d'installation dudit logiciel sur le dispositif de stockage permanent.

9. Système de contrôle de l'utilisation d'un support d'informations (103, 50), notamment magnétique ou magnéto-optique, sur un système de traitement d'informations

(100) pourvu de moyens d'identification (62, 63), mettant en oeuvre le procédé selon l'une des revendicatioqns précédentes, caractérisé en ce qu'il comprend des moyens (64, 69, 51) pour associer exclusivement ledit support d'informations (103, 50) audit système de traitement d'informations (100) de sorte que ledit support d'informations (103, 50) soit utilisable uniquement sur ledit système de traitement d'informations (100), lesdits moyens d'association exclusive étant répartis dans ledit support d'informations et dans ledit système de traitement d'informations.

10. Système selon la revendication 9, caractérisé en ce qu'au titre des moyens d'association exclusive (64, 69, 51) le système de traitement d'informations (100) comprend des moyens pour transférer sélectivement une information codée d'identification issue des moyens d'identification et traitée par des moyens d'encodage (64) dans une zone prédéterminée (51) associée et liée audit support d'informations (50).

11. Système selon la revendication 10, caractérisé en ce que l'information codée d'identification est inscrite par entrelacement avec les informations stockées sur le support d'informations, la zône prédéterminée (51) consistant en la zône de stockage physique dudit support.

12. Système selon la revendication 10, caractérisé en ce qu'au titre des moyens d'association exclusive, le support d'informations (50) comprend dans sa zône prédéterminée (51), des moyens de contrôle et de traitement (53) pour recevoir l'information codée d'identification et échanger des informations avec le système de traitement d'informations (100), fonctionnellement indépendants dudit support d'informations (50) mais physiquement liés à celui-ci.

13. Système selon la revendication 12, caractérisé en ce que les moyens de contrôle et de traitement (53)

comprennent au moins un circuit électronique intégré programmable, doté d'une mémoire, notamment un microprocesseur, et en ce que le système de traitement d'informations (100) comprend des moyens de lecture/écriture de codage (69, 64) pour échanger des informations avec ledit circuit électronique (53), ledit circuit électronique intégré étant fixé sur ledit support d'informations.

14. Système selon la revendication 13, caractérisé en ce que les moyens de lecture/écriture de codage (69, 64) comprennent une mémoire volatile (64) pour stocker l'information d'identification codée générée par les moyens d'identification (62, 63), lorsque le système de traitement d'information (100) est activé.

15. Système selon la revendication 14, caractérisé en ce que le système de traitement d'information (100) comprend en outre des moyens de lecture et/ou d'écriture d'informations (61, 65, 66) pour lire et/ou écrire des informations sur le support d'informations (50, 103), les moyens de lecture/écriture d'informations (61, 65, 66) coopérant avec les moyens de lecture/écriture de codage (69) pour réaliser l'ensemble des étapes du procédé selon l'invention.

16. Système selon la revendication 15, appliqué au contrôle de l'utilisation d'un support d'informations numériques, notamment logicielles, caractérisé en ce que les moyens de lecture/écriture d'informations (61, 65, 66) et les moyens de lecture/écriture de codage (69) sont rassemblés au sein d'un dispositif lecteur (60) comprenant en outre lesdits moyens d'identification (62, 63), des moyens pour encrypter/désencrypter (67) des logiciels stockés sur le support d'informations et des moyens (68) pour décompacter lesdits logiciels.

17. Système selon l'une des revendications 13 à 16, caractérisé en ce que le circuit électronique programmable (53) associé au support est agencé pour autoriser un nombre

prédéterminé de mises en oeuvre de l'étape d'association exclusive de l'étape d'installation.

18. Système selon l'une des revendications 9 à 15, appliqué au contrôle de l'utilisation d'un support d'informations vidéo, caractérisé en ce que les moyens d'association exclusive sont agencés pour autoriser la lecture dudit support d'informations vidéo par un nombre prédéterminé de lecteurs, notamment des magnétoscopes.

19. Système selon l'une des revendications 13 à 17, caractérisé en ce que le circuit électronique intégré programmable associé au support est agencé pour autoriser l'installation du contenu du support sur un nombre prédéterminé de systèmes de traitement d'informations reliés en réseau.

20. Système selon l'une des revendications 13 à 19, caractérisé en ce qu'il comprend des moyens pour effectuer un déroulement automatique des étapes du procédé de contrôle mis en oeuvre par ledit système.

FIG.1

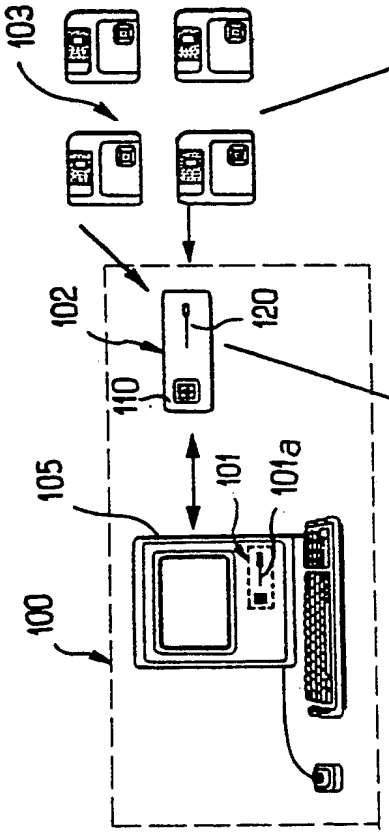


FIG.3

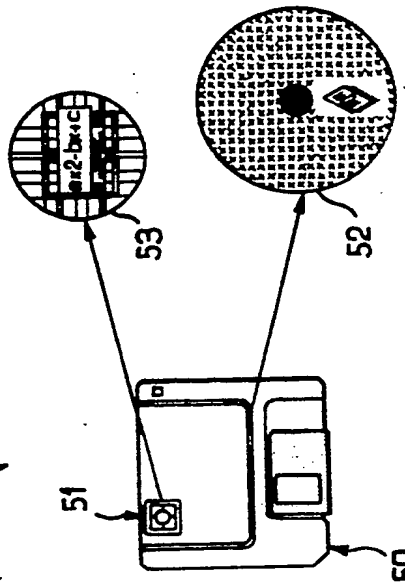
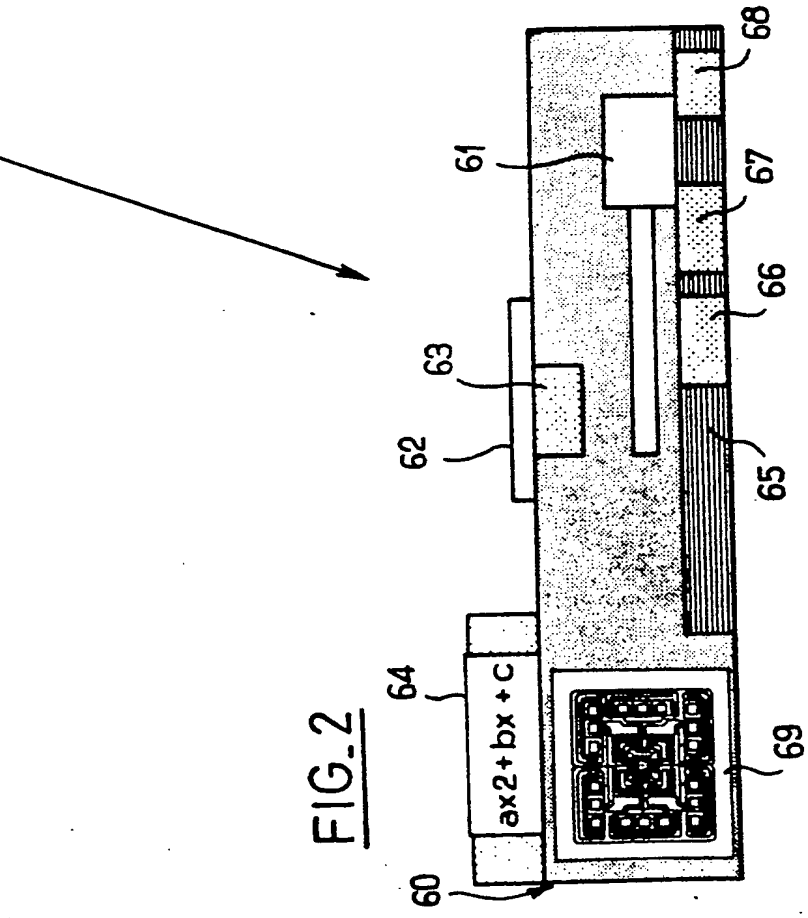


FIG.2



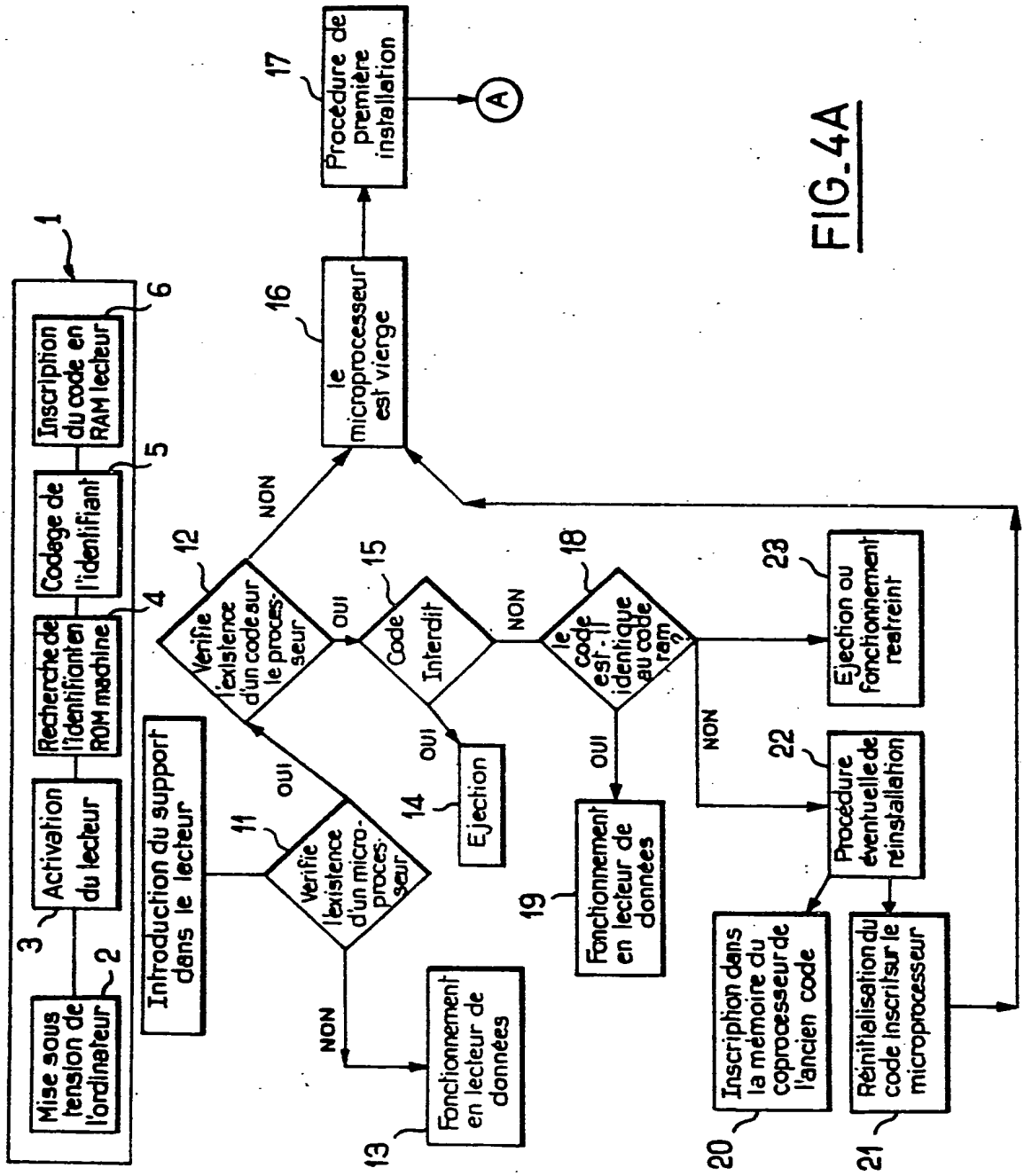


FIG_4A

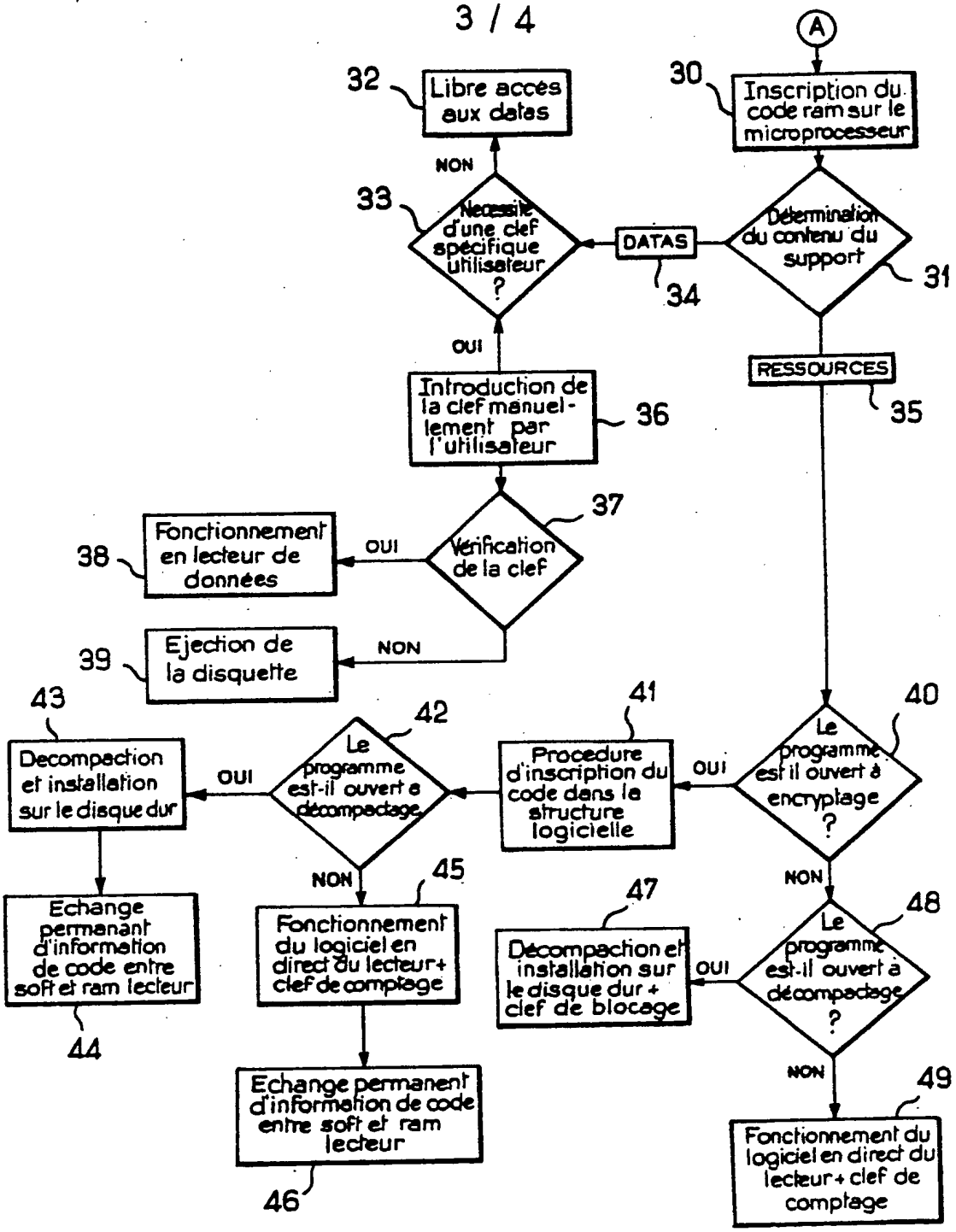


FIG_4B

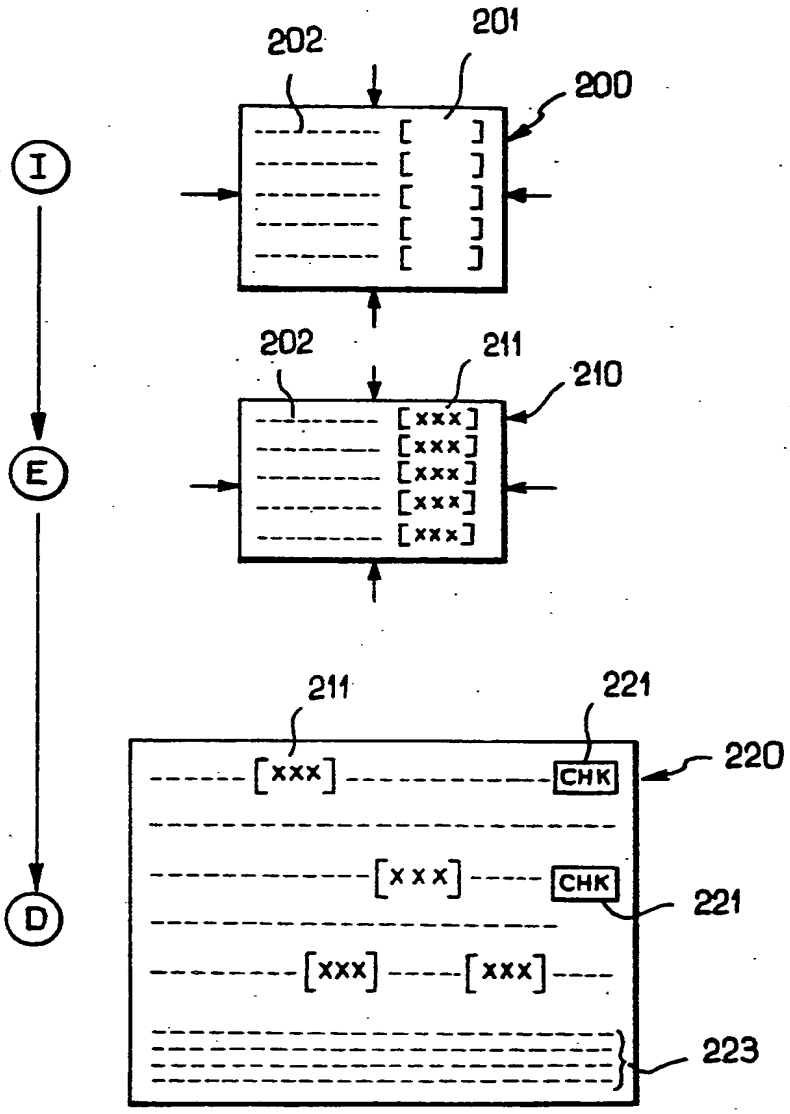


FIG_5